**Adobe Provider Data Processing Agreement: Information Security and Privacy Terms**

Effective as of September 27, 2021. These Terms replace and supersede all prior versions.

Adobe and Service Provider (the contracting entity as defined in the Agreement) have entered into an Agreement (the "Agreement") pursuant to the terms of which Service Provider may Process certain Adobe Information (as defined below) in connection with the services. This document describes the specific data transfer and processing requirements (including without limitation, the security and privacy requirements) applicable to Service Provider's Processing of Adobe Information ("Security and Privacy Procedures"). Unless specifically defined in this document, capitalized terms shall have the meanings set forth in the Agreement.

1. **Definitions.**
   - **1.1 "Adobe's Corporate Identity Provider"** means integrating with Okta as an Identity Provider (IdP) using the SAML 2.0 protocol for any user having an '@adobe.com' e-mail address (or successor technology approved by Adobe).
   - **1.2 "Adobe Customer"** means a person who either independently or on behalf of a business entity is a customer of Adobe and/or an Adobe affiliate (e.g., Magento, Marketo).
   - **1.3 "Adobe Information"** means any Adobe affiliate or Adobe Customer Confidential Information, Cardholder Information, Personal Information, or Sensitive Personal Information (including any information derived or inferred from such Adobe Information) that is Processed by Service Provider or Service Provider Parties in connection with the services. In addition to Personal Information from Adobe Customers, Adobe Information may also include Personal Information from prospects, business partners, vendors, contractors, employees, agents and advisors.
   - **1.4 "Adobe Password Standards"** means the following minimum password requirements: (i) unique user identification; (ii) minimum 12-character password; (iii) includes at least one uppercase character, one lowercase character, one digit, and one special character; (iv) must be updated every 90 days; (v) access attempts limited to six within a five-minute period; and (vi) salted and hashed.
   - **1.5 "Adobe Security Contact"** means the individual on the Adobe Information Security team that can be reached by email at scc@adobe.com in the event of a Security Incident.
   - **1.6 "Cardholder Information"** means: (i) with respect to a payment card, the account holder's name, account number, service code, card validation code/value/number, PIN or PIN block, valid to and from dates and magnetic stripe data; and (ii) information relating to a payment card transaction.
   - **1.7 "Confidential Information"** refers to that information defined as Confidential in the Agreement.
   - **1.8 "Controller"** refers to the term as defined in applicable Data Protection Requirements, including without limitation, the GDPR and the Virginia Consumer Data Protection Act (2021).
   - **1.9 "Data Protection Requirements**" means, collectively, any applicable international, national, state and local laws or regulations relating to the Processing and protection of Personal Information.
   - **1.10** "**FADP**" means the Swiss Federal Act on Data Protection of 19 June 1992 and the Swiss Ordinance on the Federal Data Protection Act of 14 June 1993, and any new or revised version thereof that may become effective from time to time.
   - **1.11** "**GDPR**" means Regulation (EU) 2016/679 of the European Parliament and of the Council.
   - **1.12 "Online Security Assessment"** means Adobe's Vendor Security Review, an online security risk assessment (or equivalent) for evaluation of Service Provider's security controls.
   - **1.13 "Personal Information"** means any information relating to an identified or identifiable natural person. An "identifiable natural person" means a person who can be identified, directly or indirectly, in

particular, by reference to an identifier such as a name, an ID number, an online identifier etc. Personal Information includes 'personal data', 'special categories of personal data' and 'sensitive personal information or data' as defined under applicable Data Protection Requirements and may relate to any individual, such as a customer, employee, vendor, or contractor.

**1.14** **"Processed" or "Processing"** means any operation or set of operations performed upon the Adobe Information or sets of Adobe Information, whether or not by automated means, such as access, collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

**1.15** **"Processor"** refers to the term as defined in applicable Data Protection Requirements, including without limitation the GDPR and the Virginia Consumer Data Protection Act (2021). "Processor" shall also include "Service Provider" as defined under the California Consumer Privacy Act (2018), as amended, where the processing activity relates to California consumers and Service Provider is processing Adobe Information on Adobe's behalf.

**1.16** **"PCI Standards"** means the security standards for the protection of payment card data with which the payment card companies require merchants to comply, including the Payment Card Industry Security Standards currently in effect and as may be updated from time to time.

**1.17** **"Public Network"** means any data network established and operated that provides data transmission services for public use, such as the Internet.

**1.18** "**Relevant Applicable Law**" means a law to which a party is subject which may require or affect the Processing of Personal Information under the Agreement which, in the case of European Personal Information (other than UK or Swiss Personal Information) shall mean any law of the European Union or a member state, in the case of UK Personal Information shall mean any law of any part of the United Kingdom and in the case of Swiss Personal Information shall mean any law of Switzerland.

**1.19** **"Secure FTP"** means "Secure File Transfer Protocol" which is a method used to encrypt and decrypt data that is transferred between a client and server, or a successor technology approved in writing by Adobe.

**1.20** **"Security Incident"** means that Service Provider reasonably believes that: a) there is a substantial likelihood of accidental or unauthorized acquisition, destruction, loss, modification, use, or disclosure of, or access to, Adobe Information Processed by, or on behalf of, Service Provider; or malware was or is present on a Service Provider system in a manner that Adobe users were or may have been exposed to the malware (for example, malware was present on a Service Provider system from which end users download content whether or not such content was downloaded).

**1.21** **"Service Provider Parties"** means any Service Provider employee, contractor, affiliate or third-party entity that Service Provider uses to provide services to Adobe under the Agreement.

**1.22** **"Sensitive Personal Information"** means an individual's: (i) social security number, national identification number or equivalent, taxpayer identification number, passport number, driver's license number or other government –issued identification number; (ii) financial account number, with or without any code or password that would permit access to the account (such as bank account numbers and debit or credit card numbers); (iii) ethnicity or race information, religious, political or philosophical belief information, medical or health information, trade union membership information, details of criminal convictions or charges, biometric or genetic information (for purpose of uniquely identifying a natural person), background check information, sex life information (including sexual orientation); (iv) Cardholder Information; (v) any Personal Information defined as "Sensitive" (or equivalent) under an applicable Data Protection Requirement.

**1.23** "**Standard Contractual Clauses**" or "**SCCs**" means:

(i) in respect of Personal Data to which the UK GDPR is applicable, the standard contractual clauses as approved by Commission Decision C(2010)593 on 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council; and

(ii) in respect of Personal Data to which the GDPR or the FADP is applicable, the standard contractual clauses for the transfer of personal data to third countries pursuant to the GDPR, adopted by the European Commission under Commission Decision (EU) 2021/914 including the text from modules 2 and 3 of such clauses and no other modules and not including any clauses marked as optional in the clauses except as otherwise specified in these Security and Privacy Procedures or the Agreement and provided that, in so far as the FADP was applicable prior to the processing by Vendor, any references in the clauses to the GDPR shall refer to the FADP;any references to "Union", "EU", and "EU Member State" shall be interpreted to mean Switzerland, Clause 17 shall be replaced to state that these Clauses are governed by the laws of Switzerland in so far as the transfers are governed by the FADP; Clause 18 shall be replaced to state, "any dispute arising from these Clauses relating to the FADP shall be resolved by the courts of Switzerland. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of Switzerland in which he/she has his/her habitual residence and the clauses shall also protect the data of legal persons until the entry into force of the revised FADP.

**1.24 "Strong Authentication"** means multi- factor authentication (e.g. something you know + something you have).

**1.25 "UK GDPR"** means Regulation (EU) 2016/679 as amended by any legislation arising out of the withdrawal of the UK from the European Union and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (as amended).

**2. Information Security Program: Technical and Organizational Measures.**

**2.1 In General.** Service Provider must:

**a.** Develop, implement, maintain, and monitor a comprehensive, written information security program that contains appropriate administrative, technical, and physical safeguards to protect against anticipated threats or hazards to the security, confidentiality, availability, or integrity of Adobe Information, including the unauthorized or accidental acquisition, disclosure, destruction, loss, alteration or use of, and the unauthorized access to, Adobe Information;

**b.** In assessing the appropriate level of security to be applied to the Adobe Information, take account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for data subjects and, in particular, ensure that additional safeguards and/or specific restrictions are applied to any Sensitive Personal Information being Processed by Service Provider;

**c.** Conduct routine risk assessments to identify and assess reasonably foreseeable internal and external risks to the security, confidentiality, availability, and integrity of electronic, paper, and other systems Processing Adobe Information and evaluate and improve, where necessary, the effectiveness of its safeguards for limiting those internal and external risks;

**d.** Ensure that its information security program is consistent with: (i) these Security and Privacy Procedures; (ii) the Data Protection Requirements; and (iii) if Service Provider has access to or otherwise Processes Cardholder Data, the PCI Standards;

**e.** If Service Provider Processes Adobe Information in any way, it shall ensure Adobe employees or Adobe administrators with access to Adobe Information are authenticated as follows: (i) Adobe users are authenticated using either Adobe's Corporate Identity Provider or Adobe Password

Standards; and (ii) all other users are authenticated via Strong Authentication or Adobe Password Standards.

**f.** Provide reasonable assistance to Adobe in Adobe's assessment and implementation of appropriate technical and organizational measures to ensure an appropriate level of security of Adobe Information.

**g.** If Service Provider transmits Adobe Information through a Public Network, Service Provider will protect it using AES-128 or equivalent encryption as defined by the most recent NIST standard, commonly implemented through protocols such as TLS, IPsec, or Secure FTP;

**h.** If Service Provider controls end user access to Adobe's network or systems, Service Provider (i) will implement industry-standard measures, including internet address protocol (IP) blocking technology, to prevent access to Adobe networks, systems, or information by users in embargoed countries (as identified in Country Group E:1 in Supplement No. 1 to Part 740 of the Export Administration Regulations (15 CFR Parts 730-774) or equivalent rules in the European Union and other jurisdictions in which Adobe and its affiliates operate).; and (ii) will notify the Adobe Security Contact immediately by email when it has reasonable "knowledge: (as defined in the Definitions of Terms in Part 772 of the Export Administration Regulations (15 CFR Parts 730-774) of any potential or actual activity involving access by users in Embargoed Countries to Adobe networks, systems, or information.

**2.2 Service Provider Review of the Information Security Program.** Service Provider shall review and update its information security program policies at least annually or whenever there is a material change in Service Provider's practices that may reasonably affect the security, confidentiality, availability, or integrity of Adobe Information. Service Provider may not alter or modify its information security program in such a way that will weaken or compromise the security of Adobe Information. If available, Service Provider will provide to Adobe (upon request) copies of its audited security assertions (SSAE18 SOC 2 Type 2 report, or, for Service Providers outside the United States, an ISO 27001 certificate, or international equivalent) on an annual basis.

**2.3 Maintaining the Information Security Program.** Service Provider shall maintain, train its workforce, and enforce its information security program at each location from which Service Provider provides the services. Service Provider shall regularly conduct network vulnerability scans, penetration testing, and incident response tabletop exercises as part of its information security program. Service Provider's information security program shall cover all networks, systems, servers, computers, notebooks, laptops, PDAs, mobile phones, and any other devices or media that Process Adobe Information or that provide access to Adobe networks or systems. Service Provider's information security program includes industry standard password protections that are equivalent to the Adobe Password Standards as appropriate, firewalls, and anti-virus and malware protections to protect Adobe Information stored on computer systems. Service Provider has baseline security configurations or hardening images for firewalls, routers, servers, personal computers, wireless and remote access points.

**2.4 Logging Requirement.** Service Provider will automatically collect system, application, and user level logs on an ongoing basis. Logs must (at a minimum) contain username, location, date and time of access, IP address, and actions performed. Logs must be kept for a minimum of ninety (90) days and made available to Adobe for review within twenty-four (24) hours upon Adobe's request (in the event of a Security Incident) or within seventy-two (72) hours for all other requests unless otherwise agreed to in writing by Adobe. Service Provider must perform audit log collection and aggregation of all key web service systems and applications that are involved in the Processing of Adobe Information and monitor those logs for evidence of any Security Incident. Authentic Copies of Adobe Information that has been

accessed or acquired by an unauthorized person must be provided promptly to Adobe Security Contact upon request.

**2.5 Adobe Security Assessments.** Adobe may require Service Provider to complete periodic Online Security Assessments of Service Provider's computing systems, environments, and networks involved in the Processing of Adobe Information. Service Provider agrees that should the Online Security Assessment reveal a material issue in Service Provider's security or privacy controls, Adobe may suspend Service Provider's access to Adobe's computing systems and networks until such the relevant security or privacy control has been appropriately addressed. Such suspension will not be considered a material breach of the Agreement.

**2.6 Magento Security, Privacy and Architecture**. To the extent Service Provider will provide services that could be integrated with or accessible from any version or type of Magento platform, server or instance (including any on-premise, cloud or open source instance of Magento), Service Provider will ensure that it maintains an equivalent or greater level of security and data protection for its systems, tools, interfaces, extensions, consoles and networks consistent with Adobe's Technical and Organizational Measures (https://www.adobe.com/go/CloudSvcsTOSM) as may be amended from time to time. Service Provider represents and warrants that it is not aware of any defect or vulnerability that could compromise the security of any Magento system, network or platform when integrated or connected with the services.

**2.7 Marketo Security, Privacy and Architecture**. To the extent Service Provider will provide services that could be integrated with or accessible from any version or type of Marketo platform, server or instance (including any on-premise, cloud or open source instance of Marketo), Service Provider will ensure that it maintains an equivalent or greater level of security and data protection for its systems, tools, interfaces, extensions, consoles and networks consistent with Marketo's Technical and Organizational Measures for Data Protection (www.adobe.com/go/marketo-dpa) as may be amended from time to time. Service Provider represents and warrants that it is not aware of any defect or vulnerability that could compromise the security of any Marketo system, network or platform when integrated or connected with the services.

**3. Processing, Disclosure, and Destruction of Adobe Information.**

**3.1 Processing.** In accordance with all Data Protection Requirements, Service Provider is a Processor or sub-processor Processing Adobe Information on Adobe's behalf. Service Provider will ensure that the Processing of Adobe Information is carried out in compliance with Adobe's instructions as further set out below.

**3.2 Processing of Adobe Information.**

**a. Scope of Processing.** If applicable, the description of the Processing carried out by Service Provider is set out in the Agreement, the Online Security Assessment, and/or Annex I and/or Appendix 1. Annex I and/or Appendix 1, if applicable, shall be populated by the parties where such information is required to be set out in these Security & Privacy Procedures under Data Protection Requirements.

**b. Purpose of Processing.** The purpose of the Processing of Adobe Information is Service Provider's provision of the services described in the Agreement.

**c. Processing Limitation.** Service Provider may only Process Adobe Information (i) on Adobe's behalf; (ii) in accordance with Adobe's written instructions (which include the Agreement and these Security and Privacy Procedures and which may be given subsequently throughout the duration of the Processing under the Agreement); and (iii) for the sole purpose of providing, operating, managing, testing, maintaining and enhancing the services and/or protecting the services from a threat to the services or to Personal Information. Service Provider is not permitted to sell Adobe Information or

cause, allow, or facilitate the sale of Adobe Information. Except as necessary to provide the services, Service Provider is not permitted to collect, retain, use, or disclose Adobe Information for its own purposes or for the purpose of any third party, firm, or enterprise (including affiliates).

**d.** If Service Provider is required, under any Relevant Applicable Law, to process any Personal Information for any purpose other than that described in these Security and Privacy Procedures or the Agreement and more particularly at c. above, Service Provider will inform Adobe of this requirement first, unless such Relevant Applicable Law(s) prohibit this on important grounds of public interest.

**e.** **Record of Processing Activities.** Service Provider and, where applicable, Service Provider Parties will maintain a written record of their Processing activities (including in electronic form) for Personal Information and Sensitive Personal Information carried out in connection with the services. Such record will include:

- i Name and contact details of the Processor or Processors and of each Controller on behalf of which the Service Provider is acting, and, where applicable, of any sub-processors (Service Provider Parties) and where applicable, of the Controller and Processor's representative, and the Processor's data protection officer;
- ii the categories of Processing carried out on Adobe's behalf;
- iii where applicable, transfers of Personal Information to a third country or an international organization, including the identification of that third country or international organization, and the documentation of appropriate safeguards;
- iv where possible, a general description of the technical and organizational security measures.

**f.** **Assistance.** In accordance with the Data Protection Requirements, Service Provider shall take all reasonable steps to assist Adobe in meeting Adobe's obligations under the Data Protection Requirements (including without limitation Articles 32 to 36 of GDPR) taking into account the nature of the Processing under the Agreement.

**g.** **Infringing instructions**. Service Provider shall immediately inform Adobe if, in its opinion, Adobe's instructions infringe the Data Protection Requirements.

**3.3 Disclosure of Adobe Information.**

**a.** **In General.** Except as may be permitted pursuant to this Section 3.3, Service Provider may not disclose Adobe Information to any third party, firm, or enterprise (including an affiliate) in violation of the terms and conditions of the Agreement or this document.

**b.** **Sub-processors.** Service Provider may use Service Provider Parties in connection with the services subject to the following requirements:

- i. Service Provider must provide Adobe with a current list of Service Provider Parties (excluding Service Provider employees) before disclosing Personal Information to any third party (including Service Provider Parties, but specifically excluding Service Provider's employees). The list must include the Service Provider Parties' country of location and instructions for communicating to Adobe any updates to this list.
- ii. Service Provider shall inform Adobe in writing of any intended changes to such list at least 15 business days in advance (together with the information necessary to enable Adobe to exercise its right to object), thereby giving Adobe sufficient time to consider such change. Where Adobe has a reasonable basis to object to a new Service Provider Party, Adobe must promptly contact Service Provider in writing within 15 business days after receipt of such change. Adobe and Service Provider will work together without unreasonable delay to

recommend an alternative arrangement. If a mutually acceptable and reasonable alternative arrangement is not found, Adobe may terminate the services without penalty.

iii. Before disclosing any Adobe Information to any Service Provider Party so as to enable it to undertake specific Processing activities on Adobe/Service Provider's behalf, Service Provider must enter into a written agreement with the Service Provider Party that contains the same data protection obligations as those imposed upon Service Provider under these Security and Privacy Procedures.

iv. At Adobe's request, Service Provider shall provide a copy of such agreement (and any subsequent amendments) to Adobe (with terms redacted as may be necessary to protect business secrets or any other confidential information).

v. Service Provider shall notify Adobe of any failure by any Service Provider Party to fulfil its obligations under such agreement.

vi. Service Provider shall ensure that the Service Provider Party complies with the obligations to which Service Provider is subject pursuant to these Security and Privacy Procedures, the Agreement and the Data Protection Requirements, and Service Provider is at all times accountable and responsible for all actions by Service Provider Parties, with respect to the disclosed Adobe Information.

vii. Service Provider shall agree a third-party beneficiary clause in its agreement with the Service Provider Party whereby, in the event that Service Provider has factually disappeared, ceased to exist in law or has become insolvent, Adobe shall be entitled to terminate Service Provider's agreement with the Service Provider Party and to instruct the Service Provider Party to destroy or return the Adobe Information.

**c. Response to Inquiries.** Service Provider must: (i) unless prohibited by a Relevant Applicable Law, notify Adobe immediately if Service Provider receives an inquiry or complaint from any individual, entity, organization, law enforcement, regulatory or governmental official or court authority related to or in connection with Adobe Information; (ii) seek to redirect the request to Adobe to the extent the request pertains to Adobe Information; (iii) where this is not possible, following prior consultation with Adobe and having obtained Adobe's consent, respond to any inquiry from law enforcement, a government official or court authority related to or in connection with Adobe Information within the time required by such official or authority; and (iv) provide reasonable support to Adobe in responding to such request in connection with Adobe Information. Unless prohibited by any Relevant Applicable Law or court order, Service Provider will notify Adobe of any anticipated disclosure to a third party. Such notification must provide Adobe with at least two (2) weeks' notice, so that Adobe or an Adobe Customer for whom Adobe processes Personal Information may, at its own expense, exercise such rights as it may have under law to prevent or limit such disclosure. Service Provider will exercise best efforts to prevent and limit any such disclosure and to preserve the confidentiality of the Adobe Information, including cooperating with Adobe to obtain an appropriate protective order or other reliable assurance that confidential treatment will be accorded to the Adobe Information.

**3.4 Destruction of Adobe Information.**

**a. In General.** If Adobe is not capable of removing or deleting Adobe Information from the services, Service Provider will, at Adobe's request or upon the expiration or termination of the Agreement for any reason, promptly return to Adobe or destroy (and certify in writing to Adobe the destruction method used, the date of destruction and the party that performed the destruction), at Adobe's option, the Adobe Information that is in Service Provider's or Service Provider Parties' possession

or control. If Adobe elects to have such information returned, Service Provider will return all such information via a bonded courier. Service Provider will destroy Adobe Information stored as a backup in accordance with its written policies and normal course of operations. If Service Provider does not have a written policy for destruction of backups, Service Provider will destroy Adobe Information stored in backup or archived form as mutually agreed between the parties. Until the Adobe Information is destroyed or returned, Service Provider shall continue to ensure compliance with these Security and Privacy Procedures.

b. **Disposal Methods.** If Service Provider disposes of any paper, electronic, or other record containing Adobe Information, Service Provider will take all reasonable steps (based on the sensitivity of the Adobe Information) to destroy the Adobe Information by: (i) shredding; (ii) permanently erasing and deleting; (iii) degaussing; or (iv) otherwise modifying the Adobe Information in such records to make it unreadable and indecipherable. All Sensitive Personal Information must be disposed of in a manner described in (i) through (iii).

4. **Cardholder Information.** This section 4 is only applicable if Service Provider will Process Cardholder Information.
   - **4.1 In General.** If Service Provider has access to (or is permitted access to) Cardholder Information, Service Provider: (i) represents that its information security program addresses the requirements of the PCI Standards; (ii) maintains a complete audit trail of all transactions and activities associated with Cardholder Information; and (iii) does not store card validation codes/values/numbers, complete magnetic stripe data or PINs and PIN blocks.
   - **4.2 PCI Certification.** If Service Provider has access to Cardholder Information, Service Provider represents and warrants that it maintains certification of its compliance with the PCI Standards and that it regularly participates in independent, third-party monthly system vulnerability scans. Service Provider will promptly provide, at the request of Adobe, current certification of compliance with the PCI Standards, by an authority recognized by the Payment Card Industry for that purpose.

5. **Personnel Security**
   - **5.1 Confidentiality.** Service Provider will ensure Service Provider Parties with access to Adobe Information or who otherwise Process Adobe Information, are informed of the confidentiality requirements and have executed confidentiality agreements or have statutory or regulatory confidentiality obligations equivalent to the requirements of these Security and Privacy Procedures.
   - **5.2 Training.** Service Provider Parties with access to or who otherwise Process Adobe Information have received appropriate training regarding information security and data privacy.
   - **5.3 Criminal History.** Service Provider will not provide access to Adobe Information to any person who, to the best of Service Provider's knowledge, has been convicted of a crime (including, without limitation, any felony or misdemeanor) involving fraud or dishonesty in the past two years.

6. **Physical and Environmental Security.** Service Provider's information processing facilities that Process Adobe Information in any format (including Adobe Information maintained in paper or digital form) are housed in secure facilities and protected by perimeter security, such as barrier access controls that provide a physically secure environment from unauthorized access, damage, and interference.

7. **Access Control**.
   - **7.1 In General.** Service Provider has established and enforces written procedures that follow role-based access control principles to control the access to systems, networks, services, and facilities that may Process or store Adobe Information. Service Provider will periodically review the users who have access

to information systems that use or house Adobe data to ensure that access privileges are relevant and appropriate for each individual user. Service Provider will make such procedures available to Adobe upon request.

**7.2 "Need to Know" Access.** Service Provider will only grant access to the Adobe Information to members of its personnel to the extent strictly necessary for providing the services and carrying out the Processing required thereunder.

**7.3 Access to Adobe Information.** Service Provider will limit access to Adobe Information to the minimum number of Service Provider Parties who require such access in order to provide the services. Access to Adobe Information must be logged and maintained for minimum ninety (90) days and made available to Adobe upon request.

**7.4 Access to Adobe Network or Systems.** If Service Provider connects to Adobe's computing systems or networks, Service Provider agrees that: (i) Service Provider will not access, and will not permit any other person or entity to access, Adobe's computing systems or networks without Adobe's authorization and any such actual or attempted access will be consistent with any such authorization; and (ii) all Service Provider connectivity to Adobe's computing systems and networks and all attempt at same will be only through Adobe's security gateways/firewalls and only for the purposes of providing the services.

**8. Communications and Operational Management.**

**8.1 In General.** Service Provider shall monitor and manage each of its information Processing facilities, including, without limitation, implementing operational procedures, change management and incident response procedures, to ensure compliance with its obligations hereunder. For any significant changes to Service Provider infrastructure, data, software, and procedures that could affect the security of the services provided to Adobe, Service Provider will communicate this to Adobe and get necessary approvals before implementing these changes to production. Service Provider shall perform regular security and vulnerability scans no less frequently than monthly and shall remediate significant vulnerabilities as soon as possible, but within 30 days of discovery (or as mutually agreed in writing between the parties).

**8.2 Anti-Malware Requirements.** Service Provider has implemented anti-malware software on all systems that Process Adobe Information to ensure that all Adobe Information is free of malware (such as viruses, Trojan horses, worms, etc.), including laptops and other devices that Process Adobe Information. For services that allow an end user to upload Adobe Information that is subsequently made available for download by an end user, Service Provider will scan the information for malware prior to making it available for download.

**8.3 Encryption.** Service Provider will encrypt all Adobe Information, using industry standard encryption tools (or better), that Service Provider: (i) transmits or receives wirelessly or across Public Networks; (ii) stores on laptops; (iii) stores on storage media (e.g. servers, databases, backup tapes); (iv) stores on portable devices (such as USB drives, mobile and tablet devices); and (v) Processes on any device that is transported outside of the physical or logical controls of Service Provider including, any printer, copier, scanner, or fax machine. Service Provider will safeguard the security and confidentiality of all encryption keys.

**8.4 Data Recovery.** Service Provider has deployed and tested back-up facilities to ensure that Adobe Information may be recovered in the event of a disaster or media failure.

**8.5 Email Notifications.** If Service Provider originates email notifications to its users, Service Provider's domain must be compliant with Sender Policy Framework (SPF) and Domain Keys Identified Mail (DKIM) protocols before January 1, 2017, or at the start of services. Service Provider is responsible for its email hygiene and Adobe shall not entertain whitelist requests. If Service Provider originates emails on behalf

of Adobe (i.e., from an "…@adobe.com" email address), Service Provider must be compliant with the Domain-based Message Authentication, Reporting and Conformance (DMARC) protocol before June 1, 2017, or at the start of services.

**9. Security Incidents.**

**9.1 In General.** Service Provider is responsible for managing Security Incidents involving Adobe Information that is Processed by, or on behalf of, Service Provider or Service Provider Parties. Service Provider will notify the Adobe Security Contact by email and by phone of any potential or actual

Security Incidents without undue delay and in any event where (i) involving Personal Information within twenty-four (24) hours of the occurrence; or (ii) involving all other Adobe Information within seventy-two (72) hours of the occurrence. Service Provider will investigate the Security Incident and take all necessary steps to eliminate or contain the exposures that led to such Security Incident. Such notification shall contain at least the following information: a description of the nature of the Security Incident (including, where possible, the categories and approximate number of data subjects and personal data records concerned); the details of a contact point where more information regarding the Security Incident may be obtained; and the likely consequences and the measures taken or proposed to be taken to address the Security Incident including to mitigate its possible adverse effects (and where it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay but in any event within the timeframes set out below ).

Service Provider must provide Adobe with a written status update, via email, within seven (7) calendar days of the occurrence of any Security Incident, detailing mitigation steps taken by Service Provider in response to such occurrence and a final report detailing the investigation and remediation within 10 business days from the close of the Security Incident (or as mutually agreed in writing between the parties). Where any Security Incident involves or may involve Personal Information, Adobe may require such notification, status update and report to be provided by Service Provider within a shorter timeframe in order for Adobe to remain in compliance with any applicable Data Protection Requirements.

**9.2 Service Provider Cooperation.** Taking into account the nature of the Processing and the information available to Service Provider, it agrees to provide (at Service Provider's sole cost) reasonable assistance and cooperation requested by Adobe, in furtherance of any correction, remediation, or investigation of a Security Incident and/or mitigation of any damage, including any notification and/or credit reporting service that Adobe may determine appropriate to send to individuals impacted or potentially impacted by such Security Incident. Unless required by law, Service Provider will not notify any individual or any third party (including any national data protection authority or equivalent regulatory body) other than law enforcement of any potential Security Incident without first consulting with and obtaining the permission of Adobe.

**10. Compliance; Right to Audit; Regulatory Requests; and Reasonable Assistance**.

**10.1 Compliance.**

**a.** Each party shall ensure that it is able to demonstrate compliance with these Security and Privacy Procedures.

**b.** Service Provider shall deal promptly and fully with any inquiries from Adobe regarding the Processing of Adobe Information in accordance with these Security and Privacy Procedures.

**c.** Service Provider shall make available to Adobe all information necessary to demonstrate compliance with the obligations set out in these Security and Privacy Procedures which stem directly from the Data Protection Requirements.

**10.2 Audits.**

**a.** Service Provider will audit the security of the computers and computing environments that it uses in Processing Personal Information for the services and the physical data centers from which Service Provider provides the services. This audit (i) will be performed at least annually; (ii) will be performed by a third-party security professional (qualified auditor) at Service Provider's selection and expertise; (iii) will result in the generation of an audit report ("Audit Report") which will be Service Provider's Confidential Information; and (iv) may be performed for other purposes in addition to satisfying this requirement (as part of a regular internal security procedure).

**b.** Upon Adobe's written request (and no more than once per year), Service Provider will provide Adobe with a confidential summary of the most recent Audit Report with respect to Service Provider's commitments in these Security and Privacy Procedures ("Summary Report") so that Adobe may reasonably verify Service Provider's compliance with these Security and Privacy Procedures. The Summary Report is Adobe Confidential Information.

**c.** Notwithstanding the above, at Adobe's request Service Provider shall permit and contribute to audits of the Processing activities, at reasonable intervals to be agreed between the parties (but no less than annually) or if there is, in Adobe's reasonable opinion, any indication of non-compliance by Service Provider. In deciding on whether to carry out an audit, Adobe may take into account any relevant certifications held by Service Provider. Adobe may conduct such audit itself or mandate an independent auditor. Any audit may include inspections at Service Provider's premises or physical facilities and shall, where appropriate, be carried out with reasonable notice.

**d.** Adobe and Service Provider shall make the information referred to in this Section 10, including the results of any audits and related reports, available to any national data protection authority or equivalent regulatory body on request.

**10.3 Impact of Audit Requirements on Standard Contractual Clauses**. In the event Standard Contractual Clauses are applicable, nothing in this Section 10 varies, modifies, or affects the Standard Contractual Clauses.

**10.4 Reasonable Assistance: Correction, deletion, and blocking of data**. To the extent Adobe does not have the ability to access Personal Information to respond to requests from individuals enforcing their right to correct, amend, port, or delete their data upon request (as permitted by Data Protection Requirements), Service Provider will assist Adobe with any reasonable request to do so within 7 business days of Adobe's request and at all times acting in compliance with Adobe's instructions. If an individual should communicate directly with the Service Provider to request enforcement of their individual rights under Data Protection Requirements in connection with the services provided to Adobe by Service Provider, Service Provider will promptly notify Adobe of the request and will provide Adobe with reasonable assistance in processing any such request (without responding to such request itself unless authorized in writing to do so by Adobe).

**11. International Data Transfers and Processing of Personal Information.**

**11.1 Transfer of European Personal Information (if applicable).** If Service Provider Processes any Personal Information that is subject to the GDPR, the UK GDPR and/or data protection laws in Switzerland, and any successors or amendment thereto ("European Personal Information") outside of the European Union or European Economic Area or any country deemed adequate by the European Commission (a "Third Country"), Service Provider shall only do so with Adobe's prior written consent and in accordance

with its written instructions and, where such prior written consent is granted, Service Provider will, for the duration of the Processing of European Personal Information:

**a.** in respect of any transfers that are subject to the GDPR or the FADP:

i. comply with the appropriate module of the Standard Contractual Clauses (either as a Processor where Adobe and/or its affiliates are Controllers or as a sub-processor where Adobe and/or its affiliates have entered into SCCs with other Adobe affiliates or Adobe customers) which Standard Contractual Clauses are hereby incorporated by reference into these Security and Privacy Procedures and the Agreement subject to the provisions of this Section 11.1.a. below; or

ii. where the GDPR is applicable to the Processing by Service Provider and Service Provider, to the extent permitted by Section 3.3, proposes to transfer European Personal Information to a third party such as a Service Provider Party in a Third Country, enter into the appropriate module (being module 3) of the SCCs directly with such third party.

For the purposes of the Standard Contractual Clauses that apply pursuant to Section 11.1.a.(i), the parties agree as follows:

(a) the text from module 2 of the Standard Contractual Clauses shall apply where Adobe and/or its affiliates are the Controller and the text from module 3 of the Standard Contractual Clauses shall apply where Adobe is a Processor on behalf its customers or other Adobe affiliates;

(b) for the purposes of clause 9(a) of the Standard Contractual Clauses, as applicable under modules 2 and 3, [option [2] applies with [15] business days as the specified time period for submitting the request for specific authorization]. Any request pursuant to clause 9(a) of the Standard Contractual Clauses shall be submitted to DPO@adobe.com together with a description of the Processing by each such sub-processor, categories of data subjects and the categories of Personal Data Processed, and the location of the Processing of Personal Data as well as any other information necessary to enable Adobe to decide on the authorization. The list of sub-processors authorized by Adobe required by Annex III of the Standard Contractual Clauses is set out in Annex III of these Security and Privacy Procedures;

(c) the information required by Annex I of the Standard Contractual Clauses is as set out in Annex I to these Security and Privacy Procedures and the signatures for the purpose of Annex IA of the Standard Contractual Clauses are the signatures to the Agreement and the date is the date of the Agreement;

(d) the technical and organizational measures required by Annex II of the Standard Contractual Clauses and the information in relation to the technical and organizational measures in relation to data subject rights as required by clause 10(b) of the Standard Contractual Clauses as applicable under modules 2 and 3 are as set out in these Security and Privacy Procedures;

(e) any notice provided under clauses 9(d), 14e and 16 of the Standard Contractual Clauses shall be provided to DPO@adobe.com and, in the case of 9(d) according to the timing set out in clause 3.3b.(v) these Security and Privacy Procedures; and

(f) for the purposes of clause 17 of the Standard Contractual Clauses, option 1 applies and the Standard Contractual Clauses shall be governed by the laws of Ireland and for the purposes of clause 18 of the Standard Contractual Clauses, the courts of Ireland shall have jurisdiction in relation to the Standard Contractual Clauses.

The parties also agree to comply with the supplementary measures set out in Annex IV, which are used to provide appropriate safeguards for transfers of Personal Data subject to the GDPR.

**b.** In respect of any transfers that are subject to the UK GDPR, comply with the Standard Contractual Clauses, which are hereby incorporated by reference into these Security and Privacy Procedures and the Agreement subject to the provisions of this Section 11.1(b) below, and the parties agree that signature to and dating of the Agreement shall constitute all required signatures and dates for the Standard Contractual Clauses.

For the purposes of the Standard Contractual Clauses that apply pursuant to Section 11.1(b), the parties agree as follows:

i. any rights to audit, pursuant to clauses 5(f) and 12(2) of the Standard Contractual Clauses, will be exercised in accordance with Section 10.2 of these Security and Privacy Procedures;
ii. that the law governing such Standard Contractual Clauses shall be the law of England and Wales;
iii. the information as required by Appendix 1 of the Standard Contractual Clauses is as set out in Appendix 1 to these Security and Privacy Procedures; and
iv. the technical and organizational measures required by Appendix 2 of the Standard Contractual Clauses are as set out in these Security and Privacy Procedures.

In the event that: (1) the Standard Contractual Clauses referred to at 11.1(b) are no longer valid for use under Article 46 of the UK GDPR; and (2) the Information Commissioner issues standard data protection clauses under s.119A(1) of the Data Protection Act 2018 which incorporate and modify the Standard Contractual Clauses at 11.1(a) to be effective under the laws of the United Kingdom ("New UK Standard Contractual Clauses"); then the parties agree that the New UK Standard Contractual Clauses shall apply to UK personal data, from such date as Adobe notifies to Service Provider, with the details of the Parties, Annexes and modules as specified at 11.1(a), but with the governing law and jurisdiction being the laws of England & Wales. The parties agree that Adobe may, by notice to the Service Provider, make any further amendments to the application of the New Standard Contractual Clauses as Adobe deems reasonably necessary in order to implement such replacement standard contractual clauses.

**c.** The parties may agree to other mechanisms to transfer European Personal Information to Third Countries, such as mechanisms contained in GDPR (Regulation (EU) 2016/679), as approved by the European Commission or another mechanism approved under applicable Data Protection Requirements, so long as such mechanism remains lawful in accordance with the decisions of the Court of Justice of the European Union and other applicable Data Protection Requirements. Adobe may, at no cost, suspend or require Service Provider to suspend, any transfers of Personal Information which in Adobe's reasonable opinion do not comply or which cease to comply with Data Protection Requirements. In such case the parties shall negotiate in good faith a solution to enable the transfers of Personal Information to be reinstated in compliance with Data Protection Requirements. If Adobe and Service Provider (and any sub-processor, where relevant) are unable to promptly agree a solution, then Adobe shall have the right to terminate the Agreement in whole or in part by providing Service Provider written notice of termination which shall be effective as of the date of such notice of termination or such later date as determined by Adobe. The parties

acknowledge and agree that a failure or a delay by Adobe to exercise its rights under this Section shall not constitute a waiver of these rights and does not prevent or restrict Adobe from exercising or further exercising its rights under this Section. No single or partial exercise of the rights under this Section shall prevent or restrict the further exercise of such rights.

**11.2 All Other Transfers**. If Service Provider accesses or Processes any Personal Information related to individuals outside of the EU/EEA/UK that is subject to data transfer requirements, Service Provider will reasonably cooperate with Adobe to establish appropriate transfer mechanisms for such transfers.

**11.3 Processing Personal Information.** Service Provider agrees that it will only Process Personal Information to the extent necessary to perform its obligations under the Agreement (and not for any other purpose) and in compliance with applicable Data Protection Requirements. Service Provider shall take all appropriate legal, organizational and technical measures to comply with its obligations under this Section 11.3 and applicable Data Protection Requirements, in particular having regard to the nature of the Personal Information. Service Provider must promptly notify Adobe of any actual or alleged breach of its obligations under this Section 11.3, or any inquiry, request or complaint received in relation to the Personal Information and must comply with any directions given by Adobe in relation to the Personal Information. Service Provider shall, upon request and within a reasonable time, correct, delete, or block Personal Information from further Processing. The Service Provider will only Process the Personal Information as instructed by Adobe and its affiliates and may disclose Personal Information only to Service Provider Parties who have a need to know and will ensure that such Service Provider Parties protect Personal Information as required by this document.

**11.4 Adobe Affiliates**. Service Provider acknowledges that the provisions of this document are intended to inure to the benefit of Adobe affiliated entities (collectively **"Adobe Affiliates"**) as third-party beneficiaries of this document, and the Adobe Affiliates will be entitled to enforce such provisions against Service Provider. Service Provider further acknowledges that the Adobe Affiliates accept their third-party beneficiary rights hereunder and that such rights will be deemed irrevocable. The respective rights and obligations of Service Provider under this document shall survive the termination, expiration, or other conclusion of the Agreement.

**12. Miscellaneous**

**12.1 Service Provider Obligations.** The obligations of Service Provider under this document shall continue for so long as Service Provider continues to Process Adobe Information, even if all agreements between Service Provider and Adobe have expired or been terminated.

**12.2 Indemnification.** Service Provider shall indemnify, hold harmless, and defend Adobe, its affiliates, and its and their officers, directors, employees, agents, successors, and assigns from and against any and all claims, losses, liabilities, damages, settlements, expenses and costs (including attorneys' fees and court costs) and any and all threatened claims, losses, liabilities, damages, settlements, expenses and costs arising from, in connection with, or based on allegations of, any of the following: (A) a material violation of the requirements of this document or the Data Protection Requirements; (B) a Security Incident; (C) the negligence or willful misconduct of Service Provider, Service Provider Parties or any third party to whom Service Provider provides access to Adobe Information or systems, with respect to security or confidentiality of Adobe Information; (D) remedial action taken by Adobe as the result of a Security Incident; and (E) any other costs incurred by Adobe necessary to enforce Adobe's rights in this document. Except as otherwise provided herein, Service Provider shall be fully responsible for, and shall pay, all costs and expenses incurred by Service Provider or Service Provider Parties with respect to the obligations imposed under this document.

**12.3 Inability to Perform; Material Breach.** In the event that Service Provider is unable to comply with the obligations stated in this document or is substantial or persistent breach of any of its obligations under the Data Protection Requirements or fails to comply with a binding decision of a competent court or a national data protection authority regarding its obligations under these Security and Privacy Procedures or the Data Protection Requirements, Service Provider must promptly notify Adobe. Adobe may be entitled (at its option) to suspend the transfer of Adobe Information, require Service Provider to cease Processing relevant Adobe Information and/or immediately terminate the Agreement. Failure to materially comply with these Security and Privacy Procedures constitutes a material breach of the Agreement by Service Provider, entitling Adobe to the remedies provided for under the Agreement.

**12.4 Termination by Adobe.** Adobe may terminate the Agreement immediately as a result of a material failure by Service Provider to comply with the requirements of this document.

**12.5 Trade Compliance.** The parties agree that each may provide the other with access to information, products, technologies, or services (hereafter referred to as "Item(s)") that may be subject to the trade control laws of the United States and other national governments regardless of where the Item is received. Each party is responsible for complying with all applicable laws that may impact each party's right to import, export, or use the Items.

**12.6 Precedence**. In the event of any conflict or inconsistency between these Security and Privacy Procedures and the Standard Contractual Clauses referred to in Section 11, the Standard Contractual Clauses shall prevail.

**ANNEX I TO THE EU STANDARD CONTRACTUAL CLAUSES**
**DESCRIPTION OF PROCESSING ACTIVITIES FOR EUROPEAN PERSONAL INFORMATION (IF APPLICABLE)**

## 1. STANDARD CONTRACTUAL CLAUSES IN RESPECT OF ANY TRANSFERS THAT ARE SUBJECT TO THE GDPR

**PROCESSING DETAILS**

**A. LIST OF PARTIES**

**Data exporter:**

- **Name**: The entity or entities defined as Adobe in the Agreement to which this Annex to the Security and Privacy Procedures is annexed.
- **Address**: As provided in the Agreement to which this Annex to the Security and Privacy Procedures is annexed.
- **Contact person's name, position and contact details**: (refer to DPO)
- **Data protection officer (if applicable)**:
  Data Protection Officer - Adobe
  Adobe Systems Software Ireland Limited
  4-6 Riverwalk,
  City West Business Campus
  Dublin 24
  Ireland
  Email: dpo@adobe.com
- **Representative in the European Union**: [*N/A*]
- **Activities relevant to the data transferred under the Standard Contractual Clauses**: The receipt of the services under the Agreement.
- **Signature and date**: The signature and date of the Agreement to which this Annex to the Security and Privacy Procedures is added.
- **Role (controller/processor)**: Controller, or Processor on behalf of its customers and/or Adobe affiliates

**Data importer:**

- **Name**: The entity defined as Service Provider in the Agreement to which this Annex to the Security and Privacy Procedures is annexed.
- **Address**: As provided in the Agreement to which this Annex to the Security and Privacy Procedures is annexed.
- **Contact person's name, position and contact details**: [*Insert details of contact*]
- **Activities relevant to the data transferred under the SCCs**: The provision of the services under the Agreement.
- **Signature and date**: The signature and date of the Agreement to which this Annex is added.
- **Role (controller/processor)**: Processor (where Adobe is a Controller) or Sub-processor (where Adobe is Processor on behalf of its customers and/or Adobe affiliates)

## B. DESCRIPTION OF TRANSFER (CONTROLLER TO PROCESSOR OR PROCESSOR TO SUB-PROCESSOR TRANSFERS)

- **Categories of data subjects whose personal data is transferred**

Adobe's end users, customers, prospects, business partners, vendors, contractors, employees, agents, and advisors who are natural persons and whose Personal Data is Processed as part of the services.

- **Categories of personal data transferred**

**[TO BE COMPLETED BY SERVICE PROVIDER]**

- **Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.**

**[TO BE COMPLETED BY SERVICE PROVIDER]**

[*Insert information regarding applied restrictions of safeguards*]

- **The frequency of the transfer (e.g., whether the data is transferred on a one-off or continuous basis).**

  [Continuous basis]

- **Nature of the processing**

  [Performance of the services pursuant to the Agreement, Order Form or Statement of Work].

- **Purpose(s) of the data transfer and further processing**

  [Performance of the services pursuant to the Agreement, Order Form or Statement of Work].

- **The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period**

  The Processing will continue until the expiration or termination of the Agreement or related Order Form unless otherwise instructed by Adobe.

## C. COMPETENT SUPERVISORY AUTHORITY

Irish Data Protection Commissioner, or the competent supervisory authority will be determined as set out in the GDPR (except where the FADP was applicable to the Processing of Personal Data prior to its Processing by Service Provider, in which case the Swiss Federal Data Protection and Information Commissioner).

**ANNEX II TO THE EU STANDARD CONTRACTUAL CLAUSES (IF APPLICABLE)**

**TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA**

These measures are as set out in the Information Security and Privacy Terms.

**ANNEX III TO THE EU STANDARD CONTRACTUAL CLAUSES (IF APPLICABLE)**

**LIST OF AUTHORIZED SUB-PROCESSORS**

| **Sub-processor** | **Address** | **Contact person's name, position and contact details** | **Location of Processing of Personal Data** | **Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorized)** |
|---|---|---|---|---|
| *[Insert if relevant – if none, leave blank or insert N/A]* | *[Insert]* | *[Insert]* | *[Insert]* | *[Insert]* |

**ANNEX IV TO THE EU STANDARD CONTRACTUAL CLAUSES (IF APPLICABLE)**

**SUPPLEMENTARY MEASURES**

1. The parties shall ensure that Service Provider shall not have access to the personal data in clear-text. To ensure this:

   A. Adobe shall use strong encryption before transmission of the data to Service Provider and shall verify the identity of Service Provider;

   B. the encryption algorithm and its parameterization (e.g., key length, operating mode, if applicable) conform to the state-of-the-art and can be considered robust against cryptanalysis performed by public authorities in the recipient country taking into account the resources and technical capabilities;

   C. the strength of the encryption and key length takes into account the specific time period during which the confidentiality of the encrypted personal data must be preserved;

   D. the encryption algorithm is implemented correctly and by properly maintained software without known vulnerabilities the conformity of which to the specification of the algorithm chosen has been verified, e.g., by certification;

   E. the keys are reliably managed (generated, administered, stored, if relevant, linked to the identity of an intended recipient, and revoked); and

   F. the keys are retained solely under the control of Adobe, or by an entity trusted by Adobe in the EEA or under a jurisdiction offering an essentially equivalent level of protection to that guaranteed within the EEA;

2. The Parties shall ensure that the data is secured before transfer to Service Provider. To ensure this, Service Provider shall ensure that disclosure or unauthorized use of that additional information is prevented by appropriate technical and organizational safeguards, such as:

   A. Access control to premises and facilities

      i Measures must be taken to prevent unauthorized physical access to premises and facilities holding personal data. Measures shall include:

         (a) Access control system

         (b) ID reader, magnetic card, chip card

         (c) (Issue of) keys

         (d) Door locking (electric door openers etc.)

         (e) Surveillance facilities

         (f) Alarm system, video/CCTV monitor

         (g) Logging of facility exits/entries

   B. Access control to systems

      i Measures must be taken to prevent unauthorized access to IT systems. These must include the following technical and organizational measures for user identification and authentication:

         (a) Password procedures (incl. special characters, minimum length, forced change of password)

         (b) No access for guest users or anonymous accounts

(c) Central management of system access

(d) Access to IT systems subject to approval from HR management and IT system administrators

C. Access control to data

i Measures must be taken to prevent authorized users from accessing data beyond their authorized access rights and prevent the unauthorized [input, reading, copying, removal] modification or disclosure of data. These measures shall include:

ii Differentiated access rights

iii Access rights defined according to duties

iv Automated log of user access via IT systems

v Measures to prevent the use of automated data-processing systems by unauthorized persons using data communication equipment

D. Disclosure control

i Measures must be taken to prevent the unauthorized access, alteration or removal of data during transfer, and to ensure that all transfers are secure and are logged. These measures shall include:

(a) Compulsory use of a wholly owned private network for all data transfers

(b) Encryption using a VPN for remote access, transport and communication of data

(c) Prohibition of portable media

(d) Creating an audit trail of all data transfers

E. Input control

i Measures must be put in place to ensure all data management and maintenance is logged, and an audit trail of whether data have been entered, changed or removed (deleted) and by whom must be maintained.

ii Measures should include:

(a) Logging user activities on IT systems

(b) Ensure that it is possible to verify and establish to which bodies personal data have been or may be transmitted or made available using data communication equipment;

(c) Ensure that it is possible to verify and establish which personal data have been input into automated data-processing systems and when and by whom the data were input;

F. Job control

i Measures should be put in place to ensure that data is processed strictly in compliance with the data importer's instructions. These measures must include:

(a) Unambiguous wording of contractual instructions

(b) Monitoring of contract performance

G. Availability control

i Measures should be put in place to ensure that data are protected against accidental destruction or loss.

ii These measures must include:

(a) Ensuring that installed systems may, in the case of interruption, be restored

(b) Ensure systems are functioning, and that faults are reported

(c) Ensure stored personal data cannot be corrupted by means of a malfunctioning of the system

(d) Uninterruptible power supply (UPS)

(e) Business Continuity procedures

(f) Remote storage

(g) Anti-virus/firewall systems

H. Segregation control

i Measures should be put in place to allow data collected for different purposes to be processed separately.

(a) These should include:

1. Restriction of access to data stored for different purposes according to staff duties.

2. Segregation of business IT systems

3. Segregation of IT testing and production environments

3. Service Provider warrants and represents that it shall use its best efforts to aware of an actual or potential changes to the information that it has provided to Adobe under clause 14(c) of the EU Standard Contractual Clauses and shall advise Adobe within 48 hours of any actual or potential changes to such information.

4. Service Provider warrants and represents that:

A. it has not purposefully created back doors or similar programming that could be used to access the personal data processed in connection with the Agreement;
B. it has not purposefully created or changed its business processes in a manner that facilitates access to such personal data; and
C. law or government policy to which Service Provider is subject does not require Service Provider to create or maintain back doors or to facilitate access to such personal data; and
D. if the personal data processed by Service Provider is encrypted, Service Provider is not obliged to be in possession or to hand over the encryption key;
E. it will notify Adobe if, at any time it is unable to continue complying with this commitment and agrees that Adobe may terminate the Agreement on such notice period as is stipulated by Adobe if Service Provider breaches this provision.

5. So as to facilitate the audit right granted under clause 10.2, Service Provider warrants and represents that:

A. its access logs and other similar trails relating to access to personal data, in particular by public authorities, are and will remain tamper proof (e.g., they should be made inalterable using state of the art encryption techniques, such as hashing, and also systematically transmitted to the exporter on a periodic basis) so that the auditors can find evidence of disclosure; and

B. its access logs and other similar trails distinguish between access due to regular business operations and access due to orders or requests for access.

6. Service Provider agrees to:

A. provide the notification under clause 3.3(c) of the Information Security and Privacy Terms and 15.1 of the EU Standard Contractual Clauses before access is granted to personal data;

B. monitor any legal or policy developments that might lead to its inability to comply with its obligations under these Security and Privacy Procedures and promptly inform Adobe of any such changes and developments, if possible, ahead of their implementation.

7. Service Provider agrees that if it can no longer give the warranty at clause 14(a) of the EU Standard Contractual Clause, that it will promptly, at Adobe's written request, return the data to Adobe and suspend any further data transfers. The parties shall test this mechanism regularly to ensure that it can be applied on short notice.

8. If Service Provider receives a request for the disclosure of personal data processed in connection with the Agreement from a public authority in a third country, Service Provider shall:

   (i) assess the legality of such a request and seek to challenge any legal request that does not adhere to applicable statutory or constitutional standards;

   (ii) inform the requesting public authority of any incompatibility of the order with the safeguards contained in the EU Standard Contractual Clauses and the resulting conflict of obligations for Service Provider;

   (iii) having obtained Adobe's prior express written approval, notify the competent supervisory authority of the request prior to disclosure, unless the Service Provider is legally prohibited from doing so;

   (iv) if the Service Provider is prohibited by any Relevant Applicable Law from notifying Adobe or the competent supervisory authority, the Service Provider agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible to Adobe. The Service Provider agrees to document its best efforts in order to be able to demonstrate them on request to Adobe;

   (v) to the extent Service Provider is unable to notify Adobe prior to disclosure and Service Provider demonstrated best efforts to challenge the request, but it is still legally compelled to disclose to the public authority in a third country, Service Provider will limit the scope of the disclosure to a public authority to only information that is expressly required in the legal request;

   (vi) for the purposes of this section, best efforts do not include actions that would result in civil or criminal penalty such as contempt of court under the laws of the relevant jurisdiction.

9. If Service Provider discloses personal data in violation of these supplementary measures, Service Provider agrees to compensate data subjects for any material and non-material damage suffered.

**APPENDIX 1 to the UK STANDARD CONTRACTUAL CLAUSES (IF APPLICABLE)**

**Description of the Transfer**

The data exporter is: the entity or entities defined as Adobe in the Addendum.
The data importer is: the entity defined as Service Provider in the Addendum.

**Data exporter**

The data exporter is (please specify briefly your activities relevant to the transfer): receiving the services under the Agreement.

**Data importer**

The data importer is (please specify briefly activities relevant to the transfer): providing the services unbder the Agreement.

**Data subjects**

The personal data transferred concern the following categories of data subjects (please specify): Adobe's end users, customers, prospects, business partners, vendors, contractors, employees, agents, and advisors who are natural persons and whose Personal Data is Processed as part of the services.

**Categories of data**

The personal data transferred concern the following categories of data (please specify): **[TO BE COMPLETED BY SERVICE PROVIDER]**

**Special categories of data (if appropriate)**

The personal data transferred concern the following special categories of data (please specify): **[TO BE COMPLETED BY SERVICE PROVIDER]**

**Processing operations**

The personal data transferred will be subject to the following basic processing activities (please specify): **[TO BE COMPLETED BY SERVICE PROVIDER]**

Performance of the services pursuant to the Agreement, Order Form or Statement of Work].

**APPENDIX 2 TO THE UK STANDARD CONTRACTUAL CLAUSES (IF APPLICABLE)**

**Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):**

These measures are as set out in the Information Security and Privacy Terms.